LPR 2400.4

Effective Date: _____

Expiration Date: _____

Langley Research Center

LaRC Network Procedural Requirements

National Aeronautics and Space Administration

Table of Contents

Preface

P1. *Purpose*

The purpose of this document is to establish procedures and requirements for network access and connectivity for the Langley Research Center.

P2. *Applicability*

These requirements apply to all employees of the Langley Research Center, including contractors and subcontractors as specified in contract terms and conditions, and to all visitors and guests who require network connectivity.

P3. *Authority*

a. NPD 2800.1, Managing Information Technology

b. NPD 2810.1, NASA Information Security Policy

c. LAPD 2400.3, Langley Research Center (LaRC) Computer Networks for Data Communications

P4. *Applicable Documents*

a. NPR 2800.1, Managing Information Technology

b. NPR 2810.1, Security of Information Technology

c. LMS-CP-5518, Granting Foreign Nationals and Foreign Representatives Computer Accounts

d. LMS-CP-5519, Center Process for Requesting Information Technology Services

e. LMS-CP-5521, Center Process for Managing Facility and Large-Scale LaRCNet Connection Requests

f. LMS-CP-5696, Accessing Network Services through the Center Firewall.

g. LMS-CP-5915, Center Process for Obtaining Two-Factor Authentication Credentials and a Virtual Private Network Account (LMS-CP-5915).

P5. *Measurement/Verification*

Compliance with and effectiveness of this LPR will be measured by the percentage of time network services are available and the number of IT Security incidents for which a network vulnerability is determined to be the root cause.

P6. *Cancellation*

None

Associate Director

DISTRIBUTION:

Approved for public release via the Langley Management System; distribution is unlimited.

Chapter 1. Background

1.1 General

a. LaRCNet is the network which provides connectivity between the Center's Information Technology (IT) systems and to external systems through connections with the Agency's wide area network service provider, NASA Integrated Services Network (NISN). LaRCNet is a federal government IT resource and as such is subject to all Federal, Agency, and local laws, policies, and/or regulations. The LaRCNet infrastructure includes the physical cable plant, all network equipment (e.g., switches, routers, network management devices, etc.) as well as the Langley managed Internet Protocol (IP) address space.

b. LaRCNet is the sole authorized mechanism for connecting to any off-site network.

1.2 Network Architecture

The LaRCNet infrastructure has two logical sections, which are referred to as Internal and External LaRCNet.

1.2.1 Internal LaRCNet

Internal LaRCNet supports the majority of network connections within the LaRC campus. The internal LaRCNet backbone connects to various networks including device access networks, management networks, wind tunnel networks, and special project networks. The Center firewall system defines the outer-most part of Internal LaRCNet.

1.2.2 External LaRCNet

a. External LaRCNet is the collection of networks that are located outside of the Center firewall. These external networks include De-Militarized Zones (DMZs), the Wireless and Guest Network (WaGN), the Isolation Network, and the Langley Remote Access System (LaRA).

b. The DMZs provide restricted and isolated access to services that are available to communities outside of Langley. They also provide protective services to the Center's client-to-network Virtual Private network (VPN) server.

c. The WaGN provides less restrictive network access for guests and visitors.

d. The Isolation Network supports all of Langley's connections to other NASA locations and to non-NASA networks, including the Internet.

e. The LaRA system allows remote devices to dial-in to the External LaRCNet.

1.3 Responsibilities

LAPD 2800.1 charters the Office of the Chief Information Officer (OCIO) as the provider of information systems, products and services that comprise the Center's Information Infrastructure. LaRCNet is a critical component of that infrastructure.

1.3.1 Information Technology (IT) Infrastructure Branch (ITIB)

Within the OCIO, the ITIB has responsibility for securely managing the development, maintenance and operation of the Langley local area network. Network support personnel work closely with the LaRC IT Security Manager (ITSM), who also resides in the ITIB.

1.3.2 Network Configuration Control Board (NCCB)

a. The NCCB is responsible for reviewing and authorizing changes to LaRCNet. The Board acts under the authority of the ITIB Head, who designates the Board Chair and members, to ensure that minimum standards are met and maintained with regard to the security, integrity, reliability, and maintainability of LaRCNet.

b. Specific membership roles and responsibilities are defined in the NCCB Charter, which is included as Appendix F.

Chapter 2. Wired Access

2.1 General

Wired access includes any connection to LaRCNet via the physical cable plant. All wired access shall be provided through the Center contract for maintenance and operation of LaRCNet.

2.2 Standard Wired Access

a. Standard wired access provides connectivity via the physical cable plant to resources residing on the Internal LaRCNet and access to resources outside the Internal LaRCNet via the Isolation Network.

b. Requests for standard wired access for desktops, servers, and printers shall be made through the requesting organization's designated Point of Contact (POC) for ordering services through the Center contract for LaRCNet maintenance and operations. Requests for this service shall follow the *Center Process for Requesting Information Technology Services* (LMS-CP-5519).

c. All other standard wired access (e.g., project or other special purpose networks) shall be provided only after review and approval by the NCCB. Requests shall be made through the requesting organization's designated POC for ordering services through the Center contract for LaRCNet maintenance and operations following the *Center Process for Managing Facility and Large-Scale LaRCNet Connection Requests* (LMS-CP-5521).

2.3 DMZ Connections

a. DMZs reside on the External LaRCNet and provide restricted and isolated access to services that are available to communities outside of Langley. DMZ networks provide connectivity to devices that must be separated from Internal LaRCNet devices because the applications they support create unacceptable risk to Internal LaRCNet resources. These networks connect to a firewall that provides customized protection and access.

b. Requests for implementation of DMZ connections shall be made through the requesting organization's designated Point of Contact (POC) for ordering services through the Center contract for LaRCNet maintenance and operations following the process defined in LMS-CP-5521. DMZ connections shall be implemented only if approved by the Center IT Security Manager or the Lead for IT Security Operations.

c. DMZ connections require firewall rules specific to the DMZ application. Firewall rule requests shall be submitted by the system Computer Security Official using the Langley IT Security Secure Site (https://rugby.larc.nasa.gov) in accordance with the process and procedures defined in LMS-CP-5696, *Accessing Network Services through the Center Firewall.*

Chapter 3. Wireless Access

3.1 General

Wireless access is provided via the Wireless and Guest Network (WaGN), which resides on the External LaRCNet. The WaGN is the only authorized wireless infrastructure within the LaRC campus and all wireless access from within the Center's physical boundaries shall be through the WaGN. The WaGN was designed to provide temporary wireless and guest network connectivity for use in conference rooms located throughout the Center.

3.2 Registration

Persons attempting wireless access shall complete the on-line registration form when prompted to do so. Accurate and complete information shall be provided.

3.3 Terms of Use

All access to the WaGN is dependent upon the user's agreement to abide by the "Terms of Use" presented during the registration process. For example, use of the WaGN network is limited to less than two weeks. A copy of the "Terms of Use" Agreement can be found in Appendix D.

3.4 Access to Internal LaRCNet Resources

Wireless access to Internal LaRCNet resources through the WaGN is restricted to computers using the Langley Virtual Private Network (VPN) provided by the OCIO. Additional information and the procedural requirements for obtaining a VPN account are provided in Chapter 5, Remote Access to Internal LaRC Resources.

Chapter 4. Connections for Langley Visitors and Guests

4.1 General

For purposes of network access, NASA civil servants and contractor personnel holding non-temporary badges issued by a NASA facility other than LaRC are considered visitors to the Center. All others (e.g., vendors and non-NASA civil servants) are considered guests.

4.2 Guests

Network connectivity for guests is restricted to Internet access and shall only be provided through the WaGN.

4.3 Visitors

The requirements in this section pertain to visitors other than foreign nationals and/or foreign representatives. If the visitor is a foreign national or foreign representative, all requests for access shall follow the process and procedures defined in LMS-CP-5518, *Granting Foreign Nationals and Foreign Representatives Computer Accounts.*

4.3.1 Access to accounts on Langley IT Systems

Visitor access to an account on a Langley IT system shall be provided only if the visitor is sponsored by a Langley civil servant. The sponsor shall provide documented proof that the following requirements have been met and shall obtain approval of account access from the Center ITSM.

a. If the visitor is a NASA civil servant, the sponsor shall ensure that the visitor has a current badge issued by a NASA facility and has a documented need to access the Langley IT system.

b. If the visitor is other than a NASA civil servant, the sponsor shall ensure that the visitor:

   (1) Has an approved National Agency Check plus Investigation (NAC-I)

   (2) Has a current badge issued by the LaRC Security and Program Protection Branch

   (3) Is not a foreign national or foreign representative

   (4) Has a documented need to access the Langley IT system

4.3.2 Connecting Non-Langley IT Systems to LaRCNet

a. LaRC connectivity for a visitor's Non-Langley IT system shall be provided only if the system and the visitor owning the system are sponsored by a Langley civil servant. The sponsor shall provide documented proof that the following requirements have been met and shall obtain approval for network access from the Center ITSM.

b. If the system owner is a NASA civil servant, the sponsor shall coordinate with the system owner to ensure that the visitor has a current badge issued by a NASA facility and:

(1) Has a documented need to connect the non-Langley system to the LaRCNet

(2) Provides documentation describing the non-Langley system's system type, make, and operating system to the Center ITSM

(3) Has obtained a valid network drop for the system through the process defined in the Center contract for maintenance and operation of LaRCNet as described in Section 2.2, Standard Wired Access

c. If the system owner is other than a NASA civil servant, the sponsor shall coordinate with the system owner to ensure that the visitor:

(1) Has an approved National Agency Check plus Investigation (NAC-I)

(2) Has a current badge issued by the LaRC Security and Program Protection Branch

(3) Is not a foreign national or foreign representative

(4) Has a documented need to connect the non-Langley system to the LaRCNet

(5) Provides documentation describing the non-Langley system's system type, make, and operating system to the Center ITSM

(6) Has obtained a valid network drop for the system through the process defined in the Center contract for maintenance and operation of LaRCNet as described in Section 2.2, Standard Wired Access

d. The sponsor shall provide documentation demonstrating that the system:

(1) Is using anti-virus software with up-to-date virus signatures and has successfully completed a virus scan within the past 24 hours

(2) Has operating system patches that are up-to-date

(3) Has been successfully and favorably scanned by the LaRC IT Security staff

Chapter 5. Remote Access to Internal LaRC Resources

5.1 General

The Langley Virtual Private Network (VPN) provides a secure means of accessing resources residing on the Internal LaRCNet while connected to another network. Use of the VPN requires Internet access and the installation of the VPN client on the workstation from which the connection is initiated. The VPN provides a secure, encrypted channel for communication between the initiating workstation and the Internal LaRCNet. Once connectivity via the VPN is established, the initiating workstation is logically connected to the LaRCNet behind the Center firewall.

5.2 Obtaining Access

a. If broadband Internet access is not available, dial-in access to External LaRCNet can be provided through the Langley Remote Access (LaRA) system. Requests for this service shall follow the process defined in LMS-CP-5519.

b. All access from non-LaRC networks and from the WaGN to resources residing on Internal LaRCNet shall be through the Langley Virtual Private Network (VPN).

c. Two-factor authentication is required to establish VPN connectivity, therefore possession of an RSA SecurID token is required prior to obtaining a VPN account.

d. All requests for SecurID tokens and VPN accounts shall be through the *Center Process for Obtaining Two-Factor Authentication Credentials and a Virtual Private Network Account* (LMS-CP-5915).

Chapter 6. Backend Network Connections

6.1 General

A Backend Network is one that provides no physical or logical connectivity to either Internal or External LaRCNet for any device that resides on that network. Backend networks may use the LaRCNet cable plant to interconnect devices only to the extent that the segment(s) of the cable plant used are physically separate from any used by Internal or External LaRCNet. All such use of the cable plant shall be approved by the ITIB and may be subject to charges in accordance with the terms and conditions of the current network support contract.

6.2 Network Configuration

All Backend Networks and all network attached devices on those networks shall be configured in such a way that prevents direct communications flow between Internal or External LaRCNet or any other external network.

6.3 Security Requirements

All Backend Networks and all network attached devices are subject to NASA and Center IT Security Policy as defined in NPD 2810.1 and shall meet all NASA and Center IT Security requirements as defined in NPR 2810.1.

6.4 Dual-Attached Devices

a. Dual attached devices are those that connect to both LaRCNet and a backend network. Requests for implementation of such connections shall be submitted to the NCCB for approval and shall include a complete and accurate drawing of the current configuration of the backend network.

b. Continued operation of any approved dual attached configuration shall always be subject to the following conditions:

(1) No communication shall be allowed between devices on the backend network and devices outside the backend network either directly or indirectly, including through a gateway, use of network address translation or use of port address translation.

(2) Unannounced audits may be conducted at any time by representatives of the LaRCNet NCCB to verify drawing accuracy and review services enabled on dual attached devices.

Chapter 7. Additional Connectivity Requirements

There shall be no connection between any external network to either the Internal or External LaRCNet except as provided by the OCIO through the LaRCNet Isolation Network. This includes connections to other NASA Centers and the Internet via NISN as well as connections between LaRC and off-site Contractor facilities.

Appendix A. Glossary

Term	Definition
External LaRCNet	The collection of networks that are a part of the LaRCNet, but are outside the protection of the Center firewall.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.
Guest	Any person not holding a non-temporary badge issued by a NASA facility.
Internal LaRCNet	That portion of the LaRCNet whose outer-most boundary is the Center firewall system.
Two-factor authentication	A system using two different methods (generally something you have and something you know) to authenticate a person's identity before granting access to a resource.
Virtual Private Network (VPN)	A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.
Visitor	NASA civil servants and contractor personnel holding non-temporary badges issued by a NASA facility other than LaRC.

Appendix B. Acronym List

CIO	Chief Information Officer
CP	Center Process
DMZ	De-Militarized Zone
IP	Internet Protocol
IT	Information Technology
ITIB	Information Technology Infrastructure Branch
ITSM	Information Technology Security Manager
LAPD	Langley Policy Directive
LaRA	Langley Remote Access
LMS	Langley Management System
LPR	Langley Procedural Requirements
NAC-I	National Agency Check plus Investigation
NCCB	Network Configuration Control Board
NISN	NASA Integrated Services Network
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NREN	NASA Research and Engineering Network
OCIO	Office of the Chief Information Officer
POC	Point of Contact
VPN	Virtual Private Network
WaGN	Wireless and Guest Network

Appendix C. Reference Documents

LaRC OCIO Web site at http://ocio.larc.nasa.gov/

ODIN Services List at https://www.odin.lmit.com/larc/

Appendix D. WaGN Terms of Use Agreement

Wireless Usage

Permanent Langley employees will only connect to the Public Wireless and Guest Network through a device that has a registered ODIN seat associated with it.

Guest access will be granted to temporary visitors for up to 10 working days at no charge. If access is needed beyond this period of time, the sponsoring organization must purchase an ODIN seat to support the usage.

Wireless client systems must be WiFi compliant and must utilize the IEEE 802.1b and 802.11g standards. Refer to the wireless client documentation to confirm compliance. The client must be based on the Internet Protocol, IP.

Wireless users must utilize the Service Set Identifier (SSID) obtained from ODIN and properly configure the SSID on their computer system. The system must also be configured to obtain an IP address, default gateway, and domain name service automatically using DHCP.

Wired Usage

Guests may use a designated jack for a wired connection to the Public Wireless and Guest Network if a Langley organization has purchased a seat to support that connection. These Public Wireless and Guest Network jacks are color-coded yellow.

Wired users must configure their computer system to obtain an IP address, default gateway, and domain name service automatically using DHCP.

Wireless and Wired Usage

Once the end user correctly fills out the registration and accepts the Terms of Use by clicking on "Yes, I Accept", the client device registration will be valid for twenty-four hours. When that period expires, the registration must be renewed by providing information on the registration page and accepting the terms of use again.

Network performance on the Langley Public Wireless and Guest Network is best effort. At time, clients may not be able to use the wireless system due to incompatibility, incorrect configuration, location, or other variables outside of LaRCNet network operations control.

Access to the Internet is limited to the following protocols and applications: http, https, ssh, telnet, ftp, sftp, webmail, and client-to-VPN services.

Service and capability may be limited due to NASA and Langley policy, as well as, network capacity.

Users of the Public Wireless and Guest Network are not authorized to provide services or network connectivity to other users.

Client computers connecting to the Langley Public Wireless and Guest Network must be running up-to-date anti-virus software.

Client computers connecting to the Langley Public Wireless and Guest Network must be running the latest operating system patches.

ODIN system backup service is not supported for computers on the Public Wireless and Guest Network.

Client computers may not connect to both the Langley Public Wireless and Guest Network and LaRCNet simultaneously.

Appendix E. Summary Guidance and Examples

E.1 Why These Requirements are Important

The LaRCNet is critical to the day-to-day operation of the Center. It has evolved to become the primary means of sharing information (both internal and external to the Center) for the approximately 3300 civil service and contractor employees that are part of the Center's aeronautics, atmospheric sciences and space exploration research environment. Virtually the entire Center workforce depends on the availability of a secure, responsive and reliable network for performing at least some part of their job. These requirements provide the structure for careful management of the network configuration and controlled access to network resources, which is key to delivering the consistently high quality network services the LaRC community has come to depend on.

E.2 How These Requirements Affect Your Responsibilities

Most people simply make use of the standard wired access available as a part of their desktop configuration and will have little, if any, need to have more than an awareness that these requirements do exist in the unlikely event they have a need for network service beyond what they routinely use. One likely scenario for such "non-routine" service might be the need for remote access through the VPN, in which case you'd need to understand the requirements and procedures for obtaining an RSA token and a VPN account (see LMS-CP-5915). Another could be hosting a visitor or guest needing network access. In this case, you would need to be familiar with the requirements and procedures for the visitor and guest access. See https://www.odin.lmit.com/larc/wireless/wirelessweb.htm for Internet only access through the WAGN and LMS-CP-5519 for LaRCNet access. (NOTE: Guest access is restricted to Internet only through the WAGN.)

If your responsibilities include any level of network support for your organization or you serve as an organization Computer Security Official (CSO) or Deputy CSO, you should ensure you have a good understanding of all the requirements in this document. This is particularly true if your organization has a need to provide access to a service or resource to some customer community outside the physical boundaries of the Langley campus.

E.3 Who to Contact If You Have Questions

The LaRC Network Architect, Tony Arviola, can be contacted via email at Tony.Arviola@nasa.gov or by phone at 757-864-8480.

Appendix F. NCCB Charter

The following copy of this charter is provided for convenience only. The official signed copy is maintained in NX, the LaRC Document Management System.

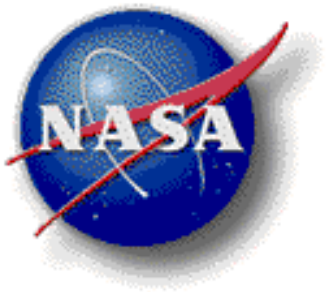
LaRCNET

Network Configuration Control Board

The Information Technology Infrastructure Branch

May 1, 2008

Revision 2



NASA Aeronautics and

Space Administration

NASA, Langley Research Center

Authorizing Signature

_____ ___/__/___

John Evans, Date

IT Infrastructure Branch,

Head

Revision History Page

Revision	Description	Date
1	Draft charter approved by NCCB Organization Team and forwarded to NCSB Head for signature and position designations	November 20, 2006
2	Team membership changes as well as branch name change	May 1, 2008

Table of Contents

1. Introduction

This document establishes the LaRCNET Network Configuration Control Board, NCCB. In addition, it defines the scope, membership roles, and basic operations of the NCCB.

2. Scope

The NCCB shall have the authority to review, approve, or disapprove all connectivity to the Langley Network. The NCCB shall create policies and processes that will be used by ITIB in managing the LaRCNet infrastructure, the connections to LaRCNet, and any ITIB managed service that utilizes LaRCNet. The NCCB may also delegate its responsibilities as it sees fit.

3. Authority

Langley policy LAPD-2810.1 designates the Office of the Chief Information Officer, OCIO, as the sole organization responsible for local area networks (LANs) at Langley. It also designates the OCIO as the organization responsible for ensuring that information technology (IT) security policies are enforced. The OCIO has delegated the management of the Langley shared LAN, LaRCNET, to the Information Technology Infrastructure Branch, ITIB. In addition, NPR-2810.1a directs each Center to institute and maintain a network configuration control board. To aid in complying with these directives as well as to promote the better management of network functionality, management, and security requirements, ITIB designates the LaRCNet NCCB as the body that will review and authorize changes to LaRCNet as well as changes to ITIB services that utilize LaRCNet.

The NCCB acts under the authority of the ITIB Head, and the ITIB Head may dissolve the NCCB at any time.

4. Purpose

The purpose of the NCCB is to assure that minimum standards are met and maintained with regards to the security, integrity, reliability, and maintainability of LaRCNet. The goal of the board is to see that network resources and services operate to meet or exceed NASA requirements while at the same time maintain an IT environment which fully supports Langley's missions and business goals.

The objectives of the NCCB are to

- Create and document processes needed to properly manage the changes to systems that are managed by the Information Technology Infrastructure Branch, ITIB;
- Create and document local policy and interpretations of Agency and Federal policies;
- Create a venue that promotes the communications between ITIB service owners and managers;
- Create processes that allow ITIB employees to perform their jobs more efficiently; Create tools and templates that will be used to support service change requests
- And create a baseline and interface description of ITIB services.

5. Membership Roles and Responsibilities

The following section describes the roles and responsibilities of key NCCB participants.

5.1. ITIB Head

The ITIB Head is responsible for

- Authorizing the NCCB to operate;
- Delegating the NCCB with the responsibilities outlined in this charter;
- Designating primary and backup members for each NCCB functional area (See Table 1.);
- Designating the NCCB chairperson and backup
- Providing the NCCB with administrative resources;
- And resolving issues involving tie votes, appeals, or situations where the OCIO must become involved.

Table 1. Voting members and their functional areas

Functional Area	**Knowledge Areas**
LaRCNet	Current network technologies and services
IT Security	IT security tools, policies (Federal, Agency, and Langley), and procedures
Back Office Systems	Back Office services and system integration
IT Services	Web and messaging service requirements and dependencies

5.2. NCCB Chairperson

The ITIB Branch head shall designate one of the four voting members as the NCCB Chair as well as designate another voting member as the backup chairperson.

The Chairperson is responsible for

- Planning, calling, and documenting NCCB meetings;
- Tracking action items;
- Monitoring action schedules;
- Assuring that change requests are acted on in a timely fashion;
- And reporting the activities of the NCCB to ITIB Branch head

5.3. Voting Members

Voting members are people who are authorized to vote on issues and queries brought before the NCCB.

Voting members of the NCCB

- Are assigned by the ITIB Branch Head;
- Must be Civil Servants;
- Must participate in all NCCB meetings;

- Must strive for an appropriate balance between functional, management, and security requirements;
- And must have sufficient business, technical, and operational expertise in their functional areas so that the implication of proposed changes can be understood from a design, technical, business, and operational perspective

5.4. Consulting members

Consulting membership is composed of representatives from each of the functional areas. The role of a consultant is to provide relevant information for all activities that come before the NCCB.

5.5. NCCB Secretary

The ITIB Head shall assign a board secretary and a backup who will take minutes of formal meetings and shall document the activities of the NCCB.

The NCCB Secretary shall document

- Network change requests;
- Formal dispositions;
- Requirements gathered by the board;
- E-mails to and from the NCCB distribution list;
- And voting proposals and voting outcomes

The board will create standard forms and templates when it deems it necessary. It will be the NCCB secretary's job to keep documentation in an accessible format and location.

Table 2 in Appendix A shows the current NCCB members as designated by the ITIB Head.

6. Quorum Definition and Voting

The physical or virtual presence of 3 members of the board shall constitute a quorum. If the primary voting member is not available, then the backup voting member for the same functional area may vote. An affirmative majority vote by a quorum of voting members shall constitute acceptance by of the proposal by the NCCB. A negative majority vote by a quorum of voting members shall constitute the rejection of the proposal by the NCCB.

Tie votes shall be delivered to the ITIB Head for resolution.

Appeals shall be presented to the ITIB Head for resolution.

7. Meetings

The NCCB meeting schedule will be determined by the NCCB Chairperson and may change based on current activities. The NCCB may also elect to use electronic means to collaborate and review material.

Appendix A. NCCB Members

Last updated May 1, 2008

The following NCCB members are designated by ITIB Head. In the event that a primary member is not available, the alternate shall act in their place.

Table 2. The current NCCB members as designated by the ITIB Head.

NCCB Role	**Designee**
LaRCNet Primary	Anthony Arviola
LaRCNet Backup	Nancy Shevlin
IT Security Primary	Kendall Freeman
IT Security Backup	M. Kim Elliott
Back Office Systems Primary	Brian McCormick
Back Office Systems Backup	
IT Services Primary	Debra Hurst
IT Services Backup	
Secretary Primary	Beth Tanner
Secretary Backup	
Chairman Primary	Anthony Arviola
Chairman Backup	Kendall Freeman